AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (CANCELLED)
2. (CANCELLED)
3. (CANCELLED)
4. (CANCELLED)
5. (CANCELLED)
6. (CANCELLED)
7. (CANCELLED)
8. (CANCELLED)
9. (CANCELLED)
10. (CANCELLED)
11. (CANCELLED)
12. (CANCELLED)
13. (CANCELLED)
14. (CANCELLED)
15. (CANCELLED)
16. (CANCELLED)
17. (CANCELLED)
18. (CANCELLED)
19. (CANCELLED)
20. (CANCELLED)
21. (CANCELLED)
22. (CANCELLED)
23. (CANCELLED)
24. (CANCELLED)

25. (CANCELLED)

26. (CANCELLED)

27. (CANCELLED)

28. (CANCELLED)

29. (CANCELLED)

30. (CANCELLED)

31. (Currently Amended) A method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes between which the mobile node is able to roam, the method comprising:

(a) generating a numerical chain comprising a series of values using a one-way coding function such that a given value within the chain is easily obtainable from a subsequent value, but the subsequent value is not easily obtainable from that given value;

(b) each time that the mobile node seeks to authenticate itself to an access node, sending a value from the numerical chain from the mobile node to an access node to which the mobile node wishes to attach, the sent value succeeding values in the chain already sent to access nodes; and

(c) using the sent value at the access node to authenticate the mobile node on the basis of a value of the numerical chain preceding the sent value in the chain,

the method further comprising, after each successful authentication, informing each of said plurality of access nodes that an authentication has been completed.

32. (Previously Presented) A method according to claim 31, wherein the comparison of the sent value and an earlier value of the numerical chain comprises comparing the output of the one-way coding function applied at least once to the sent value to an earlier value of the numerical chain.

33. (Previously Presented) A method according to claim 32, wherein the earlier value of the numerical chain is the value immediately preceding the sent value.

34. (Previously Presented) A method according to claim 33, wherein the authenticating node is the access node to which the mobile node wishes to attach.

35. (Previously Presented) A method according to claim 34, wherein the authenticating node sends a notification update to the remainder of the plurality of access nodes upon successful authentication of the mobile node.

36. (Previously Presented) A method according to claim 35, wherein the update notification is issued through a secure local multicast mechanism.

37. (Previously Presented) A method according to claim 31, wherein the authenticating node is a control node which communicates with the plurality of access nodes.

38. (Previously Presented) A method according to claim 37, wherein the authenticating node stores an update notification upon successful authentication of the mobile node.

39. (Previously Presented) A method according to claim 35, wherein the notification update comprises the sent value provided by the mobile node.

40. (Previously Presented) A method according to claim 31, wherein a value H_{i-1} of the numerical chain may be obtained from a value H_i of the numerical chain using the one-way coding function defined such that $H_{i-1} = \text{hash}(H_i)$.

41. (Previously Presented) A method according to claim 31, wherein the numerical chain is generated by providing a seed value H_n of the numerical chain, all subsequent values being obtainable through successive application of the one-way coding function.

42. (Previously Presented) A method according to claim 41, wherein the seed value H_n is based upon a value known only to the mobile node and a home network.

43. (Previously Presented) A method according to claim 41, wherein the seed value H_n is based upon a value known only to the mobile node.

44. (Previously Presented) A method according to claim 41, wherein the seed value H_n is based upon the EAP MSK or EMSK value.

45. (Previously Presented) A method according to claim 41, wherein the seed value H_n is based upon a randomly generated value.

46. (Previously Presented) A method according to claim 41, wherein the seed value is encrypted so that the access nodes cannot determine the seed value.

47. (Previously Presented) A method according to claim 31, wherein the first value of the numerical chain, obtained from successive applications of the one-way coding function to a seed value, is provided to the authenticating node by either the mobile node or a home network to which the mobile node is subscribed.

48. (Previously Presented) A method of authenticating a mobile node to a communication system, the communication system comprising a plurality of access nodes and a plurality of interfaces, the method comprising generating a plurality of numerical chains, each of the plurality of numerical chains corresponding to one of the plurality of interfaces, and a authenticating the mobile node on a plurality of the interfaces in accordance with the method of claim 31.

49. (Previously Presented) A method according to claim 48, wherein the mobile node authenticates itself to the plurality of interfaces in parallel.

50. (Previously Presented) A method according to claim 31, wherein a value of the numerical chain is used to generate at least part of an IP address for the mobile node.

51. (Previously Presented) A method according to claim 31, wherein each numerical chain is bound to a specific MAC address corresponding to a specific access node.

52. (Previously Presented) A method according to claim 31, wherein the communication system comprises a wireless access network, and the mobile node is a wireless terminal.

53. (Previously Presented) A method of authenticating a mobile node when roaming within a communication system, the method comprising:

following handover of the mobile node from a first access node of the communication system to a second access node, authenticating the mobile node to the second access node using the method of claim 31.

54. (Previously Presented) A method according to claim 53, wherein the mobile node has been previously authenticated to the said communication system by a home network of the mobile node.

55. (Previously Presented) A method of deriving a secure authentication key when a mobile node authenticates itself to an access node in accordance with claim 31, the method comprising:

providing a first authentication key K_{S0} for use by the mobile node and a first access node;

sending a hash of the first authentication key hash(K_{S0}) to a second access node and the mobile node; and

generating a new authentication key K_{S1} in accordance with the hash hash(K_{S0}).

56. (Previously Presented) A method according to claim 55, wherein the new authentication key is generated by taking a hash of the hash hash(K_{S0}), in accordance with the function K_{S1}=hash(hash(*Kso*)).

57. (Previously Presented) A method according to claim 55, further comprising the steps of:

exchanging a first nonce N_{C1} provided by the mobile node and a second nonce N_{A1} provided by the second access node between the mobile node and the second access node; and wherein the new authentication key K_{S1} is generated in accordance with the hash of the first session key K_{S0}, the first nonce N_{C1} and the second nonce N_{A1} in accordance with the function K_{S1} = hash(hash(K_{S0}), N_{C1}, N_{A1}).

58. (CANCELLED)

59. (CANCELLED)

60. (CANCELLED)